

DETAILED ACTION

1. Preliminary Amendments, received on 16 March 2005 and 23 June 2005, have been entered into record. In the first preliminary amendment, claims 1-139 have been cancelled, and claims 140-273 have been added. In the second preliminary amendment, claims 160-273 have been cancelled.
2. Claims 140-159 are presented for examination.

Priority

3. The claim for priority from PCT/EP2003/007829 filed on 18 July 2003 is duly noted.
4. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Specification

5. The abstract of the disclosure does not commence on a separate sheet in accordance with 37 CFR 1.52(b)(4). A new abstract of the disclosure is required and must be presented on a separate sheet, apart from any other text.
6. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.
7. The disclosure is objected to because of the following informalities:

Art Unit: 2131

- a. in page 1, line 31: “reduces effectively” should read –effectively reduces–;
- b. in page 5, line 20: “and the scope of the .” is not complete;
- c. in page 5, line 23: “of-respective public keys” should read –of respective public keys–;
- d. in page 6, line 25: “CA1 11” is unclear;
- e. in page 7, line 13: “Figures 5” should read –Figure 5–;
- f. in page 8, line 8: “CPU21” should read –CPU 21–;
- g. in page 12, line 28: “step 76” should read –step 67–;
- h. in page 20, line 14: “contain an arbitrarily” should read –contain an arbitrary–;
- i. in page 27, line 6: “afirst” should read –a first–;
- j. in page 36, line 35: “independent fro” should read –independent from–.

Appropriate correction is required.

Claim Objections

8. Claims 142-143, 147-148, 151-159 are objected to because of the following informalities:

- a. In claim 142, line 9: “digital data” is unclear if it relates to “digitally encoded data” (claim 140, line 4);
- b. In claim 143, lines 3-4: “a fingerprint” is unclear if it relates to “a first fingerprint” (claim 140, line 5);

- c. In claim 145, line 3: "said plurality of user terminals" lacks antecedent basis;
- d. In claim 147, line 2: "a first list of fingerprints" is unclear if it relates to "a first list of fingerprints" (claim 140, line 4);
- e. In claim 147, line 3: "digital data" is unclear if it relates to "digitally encoded data" (claim 140, line 4);
- f. In claim 147, line 7: "sender" is unclear if it relates to "a sender" (claim 147, line 4);
- g. In claim 148, line 2: "a first fingerprint" is unclear if it relates to "a first fingerprint" (claim 140, line 5);
- h. In claim 151, line 5: "a first source" is unclear if it relates to "a first source" (claim 151, line 4);
- i. In claim 152, line 7 and claim 153, line 9: "compromised;" should read – compromised.–;
- j. In claim 154, lines 4 and 7-8: "a digital signature" is unclear if it relates to "a digital signature" (claim 154, line 3);
- k. In claim 154, line 8: "a fingerprint is unclear if it relates to "a fingerprint" (claim 154, line 5);
- l. In claim 155, line 2: "a step of" should read –a step of:–;
- m. In claim 155, line 7: "a message" is unclear if it relates to "a message" (claim 155, line 3);

- n. In claim 155, line 8: “a public network” is unclear if it relates to “a public network” (claim 155, line 4);
- o. In claim 156, line 2: “a fingerprint” is unclear if it relates to “a fingerprint” (claim 155, line 7);
- p. In claim 157, lines 1-2: “said step of attaching a fingerprint” lacks antecedent basis. It is noted that it is believed that claim 157 was meant to be dependent on claim 155 and will be treated as such for the remainder of this Office Action.
- q. In claim 158, line 2: “a fingerprint” is unclear if it relates to “a fingerprint” (claim 155, line 7) and “a message” is unclear if it relates to “a message” (claim 155, line 3);
- r. In claim 158, line 5: “received corresponding fingerprints” is unclear if it relates to “receiving said first and second fingerprint” (claim 155, line 3);
- s. In claim 158, line 6: “a fingerprint” is unclear if it relates to “a fingerprint” (claim 155, line 7);
- t. In claim 159, line 2: “a step of” should read –a step of:–;
- u. In claim 159, line 2: “fingerprint comprising” should read –fingerprint comprises–;
- v. In claim 159, lines 5-6, 8 and 9: “received list of fingerprints” is unclear if it relates to “a received list of fingerprints” (claim 159, line 3);
- w. In claim 159, line 11: “the invalid versions” lacks antecedent basis.

Appropriate correction is required.

Drawings

9. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 51, 59 (Figure 5), 907, 908 (Figure 9), 110 (Figure 10), 120, 123 (Figure 11), 132, 133 (Figure 12), 143 (Figure 13a).

10. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because:

- a. reference characters "800" and "801" have both been used to designate "digital data" (page 14, lines 10 and 11);
- b. reference character "801" has been used to designate both "digital data" (page 14, line 10) and "a second identifier" (page 14, line 17);
- c. reference character "902" has been used to designate both "recipient" (page 29, line 28) and "user terminal" (page 29, line 29).

Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be

notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 101

11. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 140 and 151 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The claims are directed to a judicial exception; as such, pursuant to the Interim Guidelines on Patent Eligible Subject Matter (MPEP 2106)), the claims must have either physical transformation and/or a useful, concrete and tangible result. The claims fail to include transformation from one physical state to another. Although, the claims appear useful and concrete, there does not appear to be a tangible result claimed. Merely storing, computing, providing (as in claim 140), obtaining and comparing (as in claim 151) would not appear to be sufficient to constitute a tangible result, since the outcome of the storing, computing, providing, obtaining and comparing steps have not been used in a disclosed practical application nor made available in such a manner that its usefulness in a disclosed practical application can be realized. As such, the subject matter of the claims is not patent eligible.

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

13. Claims 140-147 and 150-159 are rejected under 35 U.S.C. 102(b) as being anticipated by Fischer (US Patent 5,214,702).

As to claim 140, Fischer discloses a system and method for public key/signature cryptography with enhanced digital signature certification, the system and method having:

storing a first list of fingerprints (i.e. hash values) **of digitally encoded data** (i.e. certificates) (col. 8, lines 7-10; col. 19, lines 43-45);

computing a first fingerprint (i.e. presignature hash value) **for at least a part of said list of fingerprints** (i.e. ordered list) (col. 8, lines 14-17);

providing said computed first fingerprint (col. 8, lines 17-20).

As to claim 141, Fischer discloses:

obtaining one or more entries of said first list of fingerprints,
whereby said one or more entries are to be covered by said first fingerprint
(col. 29, lines 28-29);

computing a hash value on at least said obtained one or more entries
(col. 8, lines 14-17).

As to claim 142, Fischer discloses:

wherein said first list of fingerprints further comprises at least one of the following: a unique identifier (i.e. documentation) associated with each fingerprint (col. 15, lines 50-54);

a time specification (i.e. expiration date) associated with each fingerprint, whereby said time specification specifies at least one of a time of entry into said first list associated with said fingerprint or said digital data, a time of generation of said fingerprint or said digital data, or a time of provision of said fingerprint or said digital data to said server (col. 18, lines 65-68; col. 19, line 1);

a link to digital data or an association with digital data of each fingerprint (col. 10, lines 57-61).

As to claim 143, Fischer discloses:

wherein said one or more entries in said step of obtaining said computed first fingerprint further comprising at least one of a unique identifier (i.e. documentation) or a time specification (i.e. expiration date) associated with a fingerprint (col. 15, lines 50-54; col. 18, lines 65-68; col. 19, line 1).

As to claim 144, Fischer discloses:

wherein said unique identifier, said time specification, said link or said association are established and assigned by said server as part of said storing step (col. 15, lines 47-54).

As to claim 145, Fischer discloses:

wherein said step of providing said computed first fingerprint (i.e. signature) comprises attaching said first fingerprint to a message that is sent to at least one of said plurality of user terminals (col. 9, lines 37-41, 48-50).

As to claim 146, Fischer discloses:

wherein said step of providing said computed first fingerprint or said step of computing said first fingerprint further comprises signing said first fingerprint by said server (col. 9, line 68; col. 10, line 1).

As to claim 147, Fischer discloses:

receiving digital data (i.e. message) (col. 10, lines 4-5);
establishing at least one of the integrity of said digital data, the identity of a sender of said digital data and the authenticity of said sender; whereby said establishing comprises at least one of verifying a digital signature for said digital data, verifying a fingerprint associated with said digital data or sender, using a secure and trusted connection for the communication with said sender, and applying an encryption scheme for the said received digital data (col. 30, lines 4-12);

computing a hash value on at least said digital data (col. 8, lines 14-17);

adding said hash value to said first list of fingerprints (col. 19, lines 43-45).

As to claim 150, Fischer discloses:

wherein said step of providing said computed first fingerprint further comprises associating and providing at least one of a time specification, a validity period information or another identifier providing for establishing the validity of said provisioned first fingerprint (col. 18, lines 65-68; col. 19, line 1).

As to claim 151, Fischer discloses:

obtaining a first list of fingerprints of digitally encoded data (i.e. hash value) **from a first source** (col. 19, lines 43-49);

obtaining a first fingerprint (i.e. digital signature, seal) **of said list of fingerprints from a first source** (col. 29, lines 28-29);

obtaining a second fingerprint (i.e. document package) **of said list of fingerprints from a second source** (col. 29, lines 28-34);

comparing said first (i.e. J) **and said second** (i.e. K) **fingerprint** (col. 30, lines 6-7).

As to claim 152, Fischer discloses:

computing a fingerprint (i.e. hash) **of said obtained first list of fingerprints** (col. 29, line 51);

comparing said computed fingerprint and said obtained first and second fingerprints (col. 29, lines 54-58);

if at least one of said comparing steps result in different fingerprints, establishing that the data integrity of said received fingerprints or said first list of fingerprints has been compromised (col. 29, lines 19-21).

As to claim 153, Fischer discloses:

obtaining at least one of said digitally encoded data of said fingerprint list (col. 29, lines 28-29);

computing a fingerprint of said obtained digital data (col. 8, lines 14-17);

comparing said computed fingerprint with the fingerprint for said obtained digital data in said received list of fingerprints (col. 29, lines 54-58);

if said comparing step results in different fingerprints, establishing that the data integrity of said received digital data or said list of fingerprints has been compromised (col. 29, lines 19-21).

As to claim 154, Fischer discloses:

verifying a digital signature for said received first and second fingerprint (col. 29, lines 54-58);

verifying a digital signature for a received list of fingerprints (col. 29, line 51);

verifying a fingerprint associated with said received first and second fingerprint or said first and second source (col. 29, lines 54-58);

receiving a user input (i.e. inputting document) to perform at least one of said steps of verifying a digital signature (i.e. verifying genuineness) and verifying a fingerprint (col. 25, lines 64-68; col. 26, lines 1-3).

As to claim 155, Fischer discloses:

receiving said first and second fingerprint together with a message sent to said client terminal via communications media of a public network connecting said client terminals and said server (col. 10, lines 1-5);

said method further comprising a step of: attaching a fingerprint of said list of fingerprints to a message sent to another client terminal via said communications media of a public network connecting said client terminals (col. 9, lines 37-41, 48-50).

As to claim 156, Fischer discloses:

wherein said steps of obtaining said first and second fingerprint and attaching a fingerprint are accomplished automatically without an explicit request by the receiving client terminal of said message but as part of a regular communication between client terminals not established for the purpose of exchanging said first or second fingerprint (Abstract, lines 3-9; col. 9, lines 37-46).

As to claim 157, Fischer discloses:

associating and attaching at least one of a time specification, a validity period information or another identifier providing for establishing

the validity of said provisioned fingerprint (col. 18, lines 65-68; col. 19, line 1).

As to claim 158, Fischer discloses:

wherein said step of attaching a fingerprint to a message is only performed for fingerprints that are verified by said client terminal to be valid and authentic (col. 10, lines 1-8);

whereby said verification may depend on the number of successful comparing steps that were performed for said attached fingerprint with received corresponding fingerprints of mutually different and/or independent sources (col. 29, lines 59-65);

wherein said step of attaching a fingerprint further comprises signing said fingerprint by said client terminal using a private key of said client terminal (col. 9, line 68; col. 10, lines 1-4).

As to claim 159, Fischer discloses:

determining whether a received fingerprint and/or a received list of fingerprints is valid and represents the latest published version by means of associated or attached information to said received fingerprint and/or received list of fingerprints or by means of a predetermined timed schedule known to said client terminal (col. 30, lines 4-12);

if said received fingerprint and/or a received list of fingerprints is not valid, disregarding said received fingerprint and/or received list of fingerprints or requesting a fingerprint and/or a list of fingerprints from

another source to replace the invalid versions (i.e. fingerprints) (col. 29, lines 19-21).

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

15. Claims 148-149 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer as applied to claim 140 above, and in view of Corella (US 2001/0032310 A1).

As to claim 148, Fischer does not disclose:

wherein at least said steps of computing a first fingerprint and providing said computed first fingerprint are performed repeatedly according to a timed schedule, and wherein said first list of fingerprints can be augmented or continued with further entries.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Fischer, as evidenced by Corella.

Corella discloses a system and method for public key validation service, the system and method having:

wherein at least said steps of computing a first fingerprint and providing said computed first fingerprint are performed repeatedly

according to a timed schedule, and wherein said first list of fingerprints can be augmented or continued (i.e. no revocation) with further entries (0062, lines 4-7).

Given the teaching of Corella, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Fischer with the teachings of Corella by applying a fingerprint after a set amount of time. Corella recites motivation by disclosing that using a short-term disposable certificate is substantially simpler and more efficient because it is stored in volatile memory and not on disk (0061, lines 3-10). It is obvious that the teachings of Corella would have improved the teachings of Fischer by applying a new fingerprint after a set amount of time in order make the system simpler and more efficient.

As to claim 149, Fischer does not disclose:

wherein said step of providing said computed first fingerprint comprises providing or updating said first fingerprint on an hourly, daily, weekly, monthly or another regular time period basis.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Fischer, as evidenced by Corella.

Corella discloses:

wherein said step of providing said computed first fingerprint comprises providing or updating said first fingerprint on an hourly, daily, weekly, monthly or another regular time period basis (0117, lines 2-4).

Given the teaching of Corella, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Fischer with the teachings of Corella by applying a fingerprint after a set amount of time. Please refer to the motivation recited above in respect to claim 148 as to why it is obvious to apply the teachings of Corella to the teachings of Fischer.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

Art Unit: 2131

USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sarah Su/
Examiner, Art Unit 2131

/Christopher A. Revak/
Primary Examiner, Art Unit 2131